UNITED STATES DISTRICT COURT
DISTRICT OF NORTH DAKOTA

Christine Cleveland, on behalf of herself individually and all others similarly situated, Plaintiff, v. Dakota Eye Institute, LLP and Dakota Eye Institute, P.C., Defendants.	Case No. _____ **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Christine Cleveland ("Plaintiff"), on behalf of herself and all others similarly situated (the "Class Members"), brings this Class Action Complaint against Defendants, Dakota Eye Institute, LLP or Dakota Eye Institute, P.C. (collectively "Defendants"). The allegations in this Complaint are based on the personal knowledge of the Plaintiff and upon information and belief and further investigation of counsel.

NATURE OF CASE

1. Plaintiff brings this class action complaint against Defendant for its failure to properly secure and safeguard Personally Identifiable Information ("PII") and Personal Health Information ("PHI"), including individual's partial or full names, date of birth, health insurance information, medical information, and/or Social Security numbers (collectively, "Private Information").

2. Defendants operates multiple ophthalmology and optometry clinics throughout the State of North Dakota.

3. Defendants require its patients to provide their Private Information in the course of providing medical services, which it collects, maintains and otherwise stores in the normal course of business.

4. By obtaining, collecting, storing, using, and deriving benefit from Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties to those persons, and knew or should have known that it was responsible for protecting and safeguarding Plaintiff's and Class Members' Private Information from unauthorized disclosure and/or criminal hacking activity, whether intentional or inadvertent.

5. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiff and Class Members, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

6. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality and security of their Private Information.

7. Plaintiff and Class Members reasonably expected that Defendants would keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

8. Defendants, however, breached their numerous duties and obligations by failing to implement and maintain reasonable safeguards; failing to comply with industry-standard data security practices and federal and state laws and regulations governing data security; failing to properly train its employees on data security measures and protocols; failing to timely recognize and detect unauthorized third parties accessing its system and

that substantial amounts of data had been compromised; and failing to timely notify the impacted Class Members.

9. Defendants discovered that a data breach (the "Data Breach") had occurred, the date of the discovery has not been disclosed.

10. Upon information and belief, Defendants filed a notice of data breach with the U.S. Department of Health and Human Services' Office for Civil Rights as early as October 23, 2023.

11. Defendant subsequently stated in its data breach notice letter dated October 31, 2023 (the "Notice of Data Breach Letter") that stated the following:

> "Recently, DEI detected and stopped a network security incident. Someone outside of our organization temporarily gained access to our network environment. An investigation revealed that the following categories of your information may have been exposed: name, address, date of birth, social security number and medical treatment information. We maintain this information consistent with our business practices in order to facilitate the treatment of our patients."

12. According to Defendants' reports, as many as 107,143 patients or more individuals may have had their Private Information accessed, obtained, and/or exfiltrated by unauthorized third parties as part of the Data Breach.

13. In this day and age of regular and consistent data security attacks and data security breaches, in particular in the healthcare service industry, and given the sensitivity of the data entrusted to Defendants, this Data Breach is particularly egregious, foreseeable and preventable.

14. By implementing and maintaining reasonable safeguards and complying with standard data security practices, Defendants could have prevented this Data Breach or at a minimum, determined there was a Data Breach much earlier and been able secure or protect Plaintiffs and Class Members Private Information much sooner.

15. Plaintiff and Class Members are now faced with a present and imminent lifetime risk of identity theft. These risks are made all the more substantial, and significant because of the inclusion of Social Security numbers and other static Private Information.

16. PII has great value to cyber criminals and data thieves, especially Social Security numbers. As a direct cause of Defendants' Data Breach, Plaintiff's and Class Members' PII is in the hands of cyber-criminals and may be available for sale on the dark web for criminals to access and abuse at Plaintiff's expense. Plaintiff and Class Members face a current and lifetime risk of imminent identity theft or fraud directly related to the Data Breach.

17. Defendants acknowledge the imminent threat the Data Breach has caused to Plaintiff and Class Members and has assured Plaintiff and Class Members that it has "taken steps to prevent such incidents from happening in the future."

18. The modern cyber-criminal can use the data and information stolen in cyber-attacks, particularly Private Information, to assume a victim's identity when carrying out criminal acts such as:

a. Using their credit history;

b. Making financial transactions on their behalf, including opening credit accounts in their name;

c. Impersonating them via mail and/or email;

d. Stealing benefits that belong to them;

e. Committing illegal acts which, in turn, incriminate them.

19. Plaintiff's and Class Members' Private Information was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect Plaintiff's and Class Members' Private Information. Upon information and belief, Defendants unduly waited in notifying Plaintiff and Class Members regarding the Data Breach.

20. As a result of Defendants' delayed response, Plaintiff and Class Members had no idea their Private Information had been compromised, and that they were, and continue to be, at significant and imminent risk of identity theft, fraud, and various other forms of personal, social and financial harm. The risk will remain for their respective lifetimes because of Defendants' negligence.

21. Plaintiff brings this action on behalf of all persons whose Private Information was compromised because Defendant failed to:

(i) adequately protect consumers' Private Information entrusted to it,

(ii) warn its current and former patients, potential patients, and current and former employees of their inadequate information security practices, and

(iii) effectively monitor their websites and platforms for security vulnerabilities and incidents.

22. Defendant's conduct amounts to negligence and violates federal and state statutes and guidelines.

23. Plaintiff and Class Members have suffered actual, concrete, and imminent injury as a direct result of Defendants' data security failures and the Data Breach. These injuries include:

(i) the invasion of privacy;

(ii) the compromise, disclosure, theft, and imminent unauthorized use of Plaintiff's and the Class Member's Private Information;

(iii) emotional distress, fear, anxiety, nuisance and annoyance related to the theft and compromise of their Private Information;

(iv) lost or diminished inherent value of Private Information; out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time;

(v) the continued and increased risk to their Private Information, which, (a) remains available on the dark web for individuals to access and abuse; and (b) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate

measures to protect Plaintiff's and Class Members' Private Information.

24. Plaintiff seeks to remedy these harms and prevent any potential future data compromise on behalf of herself and all similarly situated persons whose Private Information was compromised and stolen as a result of the Data Breach and remains at risk due to inadequate data security.

25. Accordingly, Plaintiff, on behalf of herself and all Class Members, asserts claims for negligence, negligence *per se*, and unjust enrichment. Plaintiff seeks injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity or by law.

PARTIES

A. Plaintiff Christine Cleveland

26. Plaintiff Christine Cleveland is a citizen of the State of North Dakota at all relevant times and currently resides in Wilton, North Dakota located in Burleigh and McLean counties. Plaintiff received Defendant's Notice of Data Breach Letter on or around October 30, 2023. It is believed the Plaintiff's Private Information was provided to Defendant through her status as Defendant's patient.

27. Defendant's Notice Letter stated the following with respect to Plaintiff:

> What Happened and What Information was Involved:
>
> Recently, [Defendant] detected and stopped a network security incident. Someone outside your organization temporarily gained access to our network environment. An investigation revealed that the following categories of your information may have been exposed: name, address, date of birth, social security

> number, and medical treatment information. We maintain this information consistent with our business practices in order to facilitate the treatment of our patients. Notably, the types of information affected were different for each individual, and not every individual had all of the above listed elements exposed above.

28. Prior to this Data Breach, Plaintiff had taken steps to protect against keeping her Private Information safe and monitored her Private Information closely. Plaintiff has not knowingly transmitted her Private Information over unsecured or unencrypted internet connections.

29. Plaintiff has suffered actual damages and is at imminent, impending, and substantial risk for identity theft or fraud and future economic harm due to the highly sensitive nature of the information that was targeted and stolen in the Data Breach. Since learning about the breach, in an effort to mitigate the risk, Plaintiff has spent time and effort reviewing financial statements and identity theft protection reports to detect and prevent identity theft or fraud. Plaintiff has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the theft and compromise of her Private Information. Plaintiff will continue to spend additional time and incur future economic costs associated with the detection and prevention of identity theft or fraud.

B. Defendant Dakota Eye Institute, LLP

30. Defendant Dakota Eye Institute, LLP is a domestic limited liability partnership formed under the laws of the State of North Dakota, with its registered agent as William Marion and principal place of business located at 200 S 5th St., Bismarck, North Dakota 58504-5675 in Burleigh County.

C. Defendant Dakota Eye Institute, P.C.

31. Defendant Dakota Eye Institute, P.C. is a professional domestic corporation formed under the laws of the State of North Dakota, with its registered agent as Douglas W. Litchfield and principal place of business located at 200 S 5th St., Bismarck, North Dakota 58504-5675 in Burleigh County.

JURISDICTION AND VENUE

32. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the aggregate amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

33. This Court has personal jurisdiction over Defendant as Defendant's principal places of business is located within this District.

34. Venue is proper in this Court under 28 U.S.C. § 1391, because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District, and Defendant resides within this judicial district.

FACTUAL ALLEGATIONS

A. Background

35. In the ordinary course of doing business with Defendant collects, stores and utilizes its patients, and prospective patients Private Information which are required to provide Defendant with sensitive PII of themselves and other individuals such as:

(i) Full names;

(ii) Address;

(iii) Date of Birth;

(iv) Medical treatment information;

(v) Social Security numbers. [1]

36. Defendant Dakota Eye Institute, provides a privacy policy on its website, wherein it states that it "[uses] the personally identifiable information we collect for internal purposes."[2]

B. The Data Breach

37. As stated in its data breach notice, "Recently, [Defendants] discovered a cybersecurity incident that impacted its IT systems. Immediately upon identifying the incident, DEI engaged third-party cybersecurity experts to assess, contain, and remediate the incident. Law enforcement was also notified."

38. Defendants then made steps to secure its systems and retain independent cybersecurity experts to investigate the matter further.

39. Defendants notified its patients of the Data Breach on October 31, 2023.

40. Defendants did not disclose to Class Members when the breach was discovered. Defendants did not take any steps to notify affected Class Members until at least October 31, 2023.

[1] The North Dakota Century Code defines "personal information" as "an individual's first name or first initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted…(1) The individual's social security number…". *See* N.D.C.C. § 51-30 (4)(a) (listing data elements (1)-(10)).
[2] https://www.dakotaeye.com/privacy-policy/ (last accessed November 6, 2023)

41. Additionally, though Plaintiff and Class members have an interest in ensuring that their information remains protected, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures taken to ensure a data security breach does not occur again have not been shared with regulators or Class Members.

C. Defendant Was Aware of the Data Breach Risks

42. Defendants had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

43. Plaintiff and Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to employ reasonable care to keep such information confidential and secure from unauthorized access.

44. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the healthcare services industry preceding the date of the breach.

45. Indeed, data breaches, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendants.

46. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[3] Identity thieves use the stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[4]

47. The Private Information of Plaintiff and Class Members were taken by cyber criminals and data thieves for the very purpose of engaging in identity theft or fraud, or to sell it to other criminals who will purchase the Private Information for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

48. Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, including Social Security numbers and medical treatment information, and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members a result of a data security breach.

49. Plaintiff and Class Members now face years of constant surveillance and monitoring of their financial and personal records. The Class is incurring and will continue

---

[3] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://www.myoccu.org/sites/default/files/pdf/taking-charge-1.pdf (last visited Nov. 24, 2021).

[4] *Id*. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

to incur such damages in addition to any currently known or unknown fraudulent use of their Private Information.

50. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's own failure to implement or maintain adequate data security measures for the Private Information within its possession of Plaintiff and Class Members.

D. Defendant Failed to Comply with FTC Guidelines

51. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

52. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

53. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested

methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

54. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

55. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

56. To prevent and detect cyber-attacks, including the attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government and FTC, the following measures:

(i) Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of malware and how it is delivered;

(ii) Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication

Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing;

(iii) Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users;

(iv) Configure firewalls to block access to known malicious IP addresses;

(v) Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system;

(vi) Set anti-virus and anti-malware programs to conduct regular scans automatically;

(vii) Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary;

(viii) Configure access controls—including file, directory, and network share permissions— with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares;

(ix) Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications;

(x) Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common malware locations,

such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder;

(xi) Consider disabling Remote Desktop protocol (RDP) if it is not being used;

(xii) Use application whitelisting, which only allows systems to execute programs known and permitted by security policy;

(xiii) Execute operating system environments or specific programs in a virtualized environment; and

(xiv) Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

57. Defendants were at all times fully aware of their obligation to protect the Private Information of patients, prospective patients and employees. Defendants were also aware of the significant repercussions that would result from its failure to do so.

E. Defendant Failed to Comply with Industry Standards

58. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices. Best cybersecurity practices that are standard in the healthcare services industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring

and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

59. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness. These frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

F. PII Holds Value to Cyber Criminals

60. Businesses, such as Defendant, that store Private Information are likely to be targeted by cyber criminals and data thieves. Financial information, including credit card, bank account and routing numbers may be tempting targets for hackers, but information such as dates of birth, medical treatment information and Social Security numbers are even more attractive to cyber criminals; they are not easily destroyed or changed and can be used to perpetrate acts of identity theft and other types of fraud.

61. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials and information. For example, personal

information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[5]

62. Social Security numbers, for example, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems. [6]

63. What is more, it is no easy task, albeit near impossible to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

---

[5] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web- how-much-it-costs (last visited Apr. 7, 2021).

[6] *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Nov. 24, 2021).

64. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[7]

65. Here, the unauthorized access left the cyber criminals and data thieves with the tools to perform the most thorough identity theft—they have obtained all the essential Personal Information to mimic the identity of the victim. The Private Information of Plaintiff and Class Members stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiff and Class Members. Stolen Private Information of Plaintiff and Class Members represents essentially one-stop shopping for identity thieves

66. The FTC has released its updated publication on protecting Private Information for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct

[7] *Id.*

security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

67. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[8]

68. Companies recognize that Private Information is a valuable asset and a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other PII on a number of Internet websites. The stolen Private Information of Plaintiff and Class Members has a high value on both legitimate and black markets.

69. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or other government issues identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

[8] *See* https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29.

70. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Class Members whose Social Security numbers have been compromised now face a real, present, imminent and substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

71. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because those victims can file a dispute, cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — Social Security number, driver's license number or government-issued identification number, name, and date of birth are durable.

72. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[9]

73. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to

[9] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem- hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Apr. 7, 2021).

police. An individual may not know that their driver's license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

G. Plaintiff's and Class Members' Damages

74. Defendant has failed to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' Private Information.

75. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

76. Plaintiff and Class Members presently face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

77. Plaintiff and Class Members have been, and currently face substantial risk of being targeted now and in the future, subjected to phishing, data intrusion, and other illegality based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

78. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

79. Plaintiff and Class members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in data breach cases.

80. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

81. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach

82. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password protected.

83. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

84. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

H. Plaintiff Cleveland's Experience

85. Plaintiff Cleveland entrusted her Private Information and other confidential information to Defendants, through providing her Private Information to either Defendant

Dakota Eye Institute, LLP or Dakota Eye Institute, P.C., through her status as a patient of Defendant's. Plaintiff would not have provided her Private Information to Defendant had she known that Defendant would not take reasonable steps to safeguard her Private Information.

86. Plaintiff has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone calls, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This is time that has been lost forever and cannot be recaptured.

87. Plaintiff stores all documents containing her Private Information in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for the online accounts that she has.

88. Plaintiff has suffered actual injury in the form of damages to, and diminution in, the value of his Private Information – a form of intangible property that Plaintiff Cleveland entrusted to Defendant. This PII was compromised in, and has been diminished as a result of, the Data Breach.

89. Plaintiff has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

90. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her Private Information

resulting from the compromise of her Private Information, especially her Social Security number, in combination with his name, address, phone number, and email address, which Private Information is now in the hands of cyber criminals and other unauthorized third parties.

91. Knowing that thieves stole her Private Information, including her Social Security number and/or driver's license number and other PII that he was required to provide to Defendant through his employer, and knowing that her Private Information will likely be sold on the dark web, has caused Plaintiff great anxiety.

92. Additionally, Plaintiff does not recall having been involved in any other data breaches in which her highly confidential PII, such as Social Security Number was compromised.

93. Plaintiff has a continuing interest in ensuring that her Private Information which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

94. As a result of the Data Breach, Plaintiff is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

CLASS ACTION ALLEGATIONS

95. Plaintiff brings this nationwide class action pursuant to Federal Rules of Civil Procedure, Rules 23(b)(2), 23(b)(3), and 23(c)(4), individually and on behalf of all members of the Class:

> All natural persons residing in the United States whose Private Information was compromised in the Data Breach of Dakota Eye Institute which was disclosed on or about October 31, 2023, (the "Class").

96. Excluded from the Class are : (i) all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; (ii) defendants and their employees, officers, directors, affiliates, parents, and any entity in which Defendant has a whole or partial ownership of financial interest; (iii) any counsel and their respective staff appearing in this matter; and (iv), and all judges assigned to hear any aspect of this litigation, their immediate family members, and respective court staff.

97. Plaintiff reserves the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

98. **Numerosity**. The Class is so numerous that joinder of all members is impracticable. The Class includes thousands of individuals whose personal data was compromised by the Data Breach. The exact number of Class Members is in the possession and control of Defendants and will be ascertainable through discovery, but Defendants has disclosed that approximately 107,143 individuals' Private Information was involved in the Data Breach.

99. **Commonality.** There are numerous questions of law and fact common to Plaintiff and the Class that predominate over any questions that may affect only individual Class Members, including, without limitation:

(i) Whether Defendants unlawfully maintained, lost or disclosed Plaintiff's and Class Members' Private Information;

(ii) Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

(iii) Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

(iv) Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

(v) Whether Defendants owed a duty to Class Members to safeguard their Private Information;

(vi) Whether Defendants breached duties to Class Members to safeguard their Private Information;

(vii) Whether cyber criminals obtained Class Members' Private Information in the Data Breach;

(viii) Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;

(ix) Whether Defendants owed a duty to provide Plaintiff and Class Members timely notice of this Data Breach, and whether Defendants breached that duty;

(x) Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

(xi) Whether Defendant's conduct was negligent;

(xii) Whether Defendant's conduct violated federal law;

(xiii) Whether Defendant's conduct violated state law; and

(xiv) Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

100. **Typicality**. Plaintiff's claims are typical of the claims of the Class in that Plaintiff, like all Class Members, had her personal data compromised, breached, and stolen in the Data Breach. Plaintiff and all Class Members were injured through the uniform misconduct of Defendants, described throughout this Complaint, and assert the same claims for relief.

101. **Adequacy**. Plaintiff and counsel will fairly and adequately protect the interests of the Class. Plaintiff retained counsel who are experienced in Class action and complex litigation. Plaintiff has no interests that are antagonistic to, or in conflict with, the interests of other Class Members.

102. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiff and Class Members have been harmed by Defendant's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to

Defendant's conduct and/or inaction. Plaintiff knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

103. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each Class Member. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing Defendants to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by Class Members would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

104. Class certification, therefore, is appropriate under Rule 23(a) and (b)(2) because Defendants has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

105. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of

which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

(i) Whether Defendants owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

(ii) Whether Defendants breached a legal duty to Plaintiff and the Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

(iii) Whether Defendants failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

(iv) Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

(v) Whether Plaintiff and Class Members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

106. Plaintiff re-alleges and incorporates by reference herein all of the previous allegations contained herein.

107. Plaintiff and Class Members entrusted Defendants with their Private Information as a condition of receiving healthcare services from Defendants.

108. Plaintiff and Class Members entrusted their Private Information to Defendants through their employer on the premise and with the understanding that Defendants would safeguard their information, use their Private Information for business purposes only, and not disclose their Private Information to unauthorized third parties.

109. Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, using, and protecting their Private Information from unauthorized third parties.

110. The legal duties owed by Defendants to Plaintiff and the Class Members include, but are not limited to the following:

(i) To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information of Plaintiff and Class Members in their possession;

(ii) To protect Private Information of Plaintiff and Class Members in their possession using reasonable and adequate security

procedures that are compliant with industry-standard practices; and

(iii) To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Class members of the Data Breach.

111. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the Federal Trade Commission, the unfair practices by companies such as Defendant of failing to use reasonable measures to protect Private Information.

112. Various FTC publications and data security breach orders further form the basis of Defendant's duty. Plaintiff and Class Members are consumers under the FTC Act. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and by not complying with industry standards.

113. Defendants breached its duties to Plaintiff and Class Members. Defendant knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the fact that data breaches have recently been prevalent.

114. Defendants knew or should have known that its security practices did not adequately safeguard the Private Information of Plaintiff and Class Members.

115. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect the PII of Plaintiff and Class Members from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiff and Class Members during the period it was within Defendant's possession and control.

116. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiff and Class Members. That special relationship arose because Plaintiff and Class Members entrusted Defendants with their confidential PII, a necessary part of obtaining services from Defendanst.

117. Defendants was subject to an "independent duty," untethered to any contract between Defendants and Plaintiff.

118. Defendant's own conduct created a foreseeable risk of harm to a foreseeable individual, including Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decisions not to comply with industry standards for safekeeping of the Private Information of Plaintiff and Class Members, including basic encryption techniques freely available to Defendants.

119. Defendants were in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

120. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and Class Members.

121. Defendants breached the duties it owes to Plaintiff and Class Members in several ways, including:

(i) Failing to implement adequate security systems, protocols, and practices sufficient to protect patients' Private Information and thereby creating a foreseeable risk of harm;

(ii) Failing to comply with the minimum industry data security standards during the period of the Data Breach;

(iii) Failing to act despite knowing or having reason to know that its systems were vulnerable to attack; and

(iv) Failing to timely and accurately disclose to patients and employees that their Private Information had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

122. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and Class Members and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The Private Information of Plaintiff and Class Members was stolen and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

123. Due to Defendant's conduct, Plaintiff and Class Members are entitled to credit monitoring. The Private Information taken can be used for identity theft and other types of financial fraud against the members of the proposed Class.

124. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year.

125. As a result of Defendant's negligence, Plaintiff and Class Members suffered injuries that include:

(i) the lost or diminished value of Private Information;

(ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;

(iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account;

(iv) the continued risk to their Private Information, which may remain for sale on the dark web and is in Defendant's possession and subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession;

(v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members, including ongoing credit monitoring.

126. These injuries were reasonably foreseeable given the history of security breaches of this nature in the financial sector. The injury and harm that Plaintiff and Class Members suffered was the direct and proximate result of Defendant's negligent conduct.

COUNT II
NEGLIGENCE PER SE

127. Plaintiff re-alleges and incorporates by reference herein all of the previous allegations contained herein.

128. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

129. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's nature, including, specifically, the immense damages that would result to Plaintiff and Class Members due to the valuable nature of the PII at issue in this case—including Social Security numbers.

130. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

131. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

132. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

133. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to:

(i) actual identity theft;

(ii) the compromise, publication, and/or theft of their PII;

(iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII;

(iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft;

(v) costs associated with placing freezes on credit reports;

(vi) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so

long as Defendants fail to undertake appropriate and adequate measures to protect the PII of its current and former employees and patients in its continued possession; and

(vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

134. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

COUNT III
UNJUST ENRICHMENT

135. Plaintiff re-alleges and incorporates by reference herein all of the previous allegations contained herein.

136. Defendants benefited from receiving Plaintiff's and Class members' PII by its ability to retain and use that information for its own financial business benefit. Defendant understood this benefit.

137. Defendants also understood and appreciated that Plaintiff and Class Members' PII was private and confidential, and its value depended upon Defendants maintaining the privacy and confidentiality of that PII.

138. Plaintiff and Class Members conferred a monetary benefit upon Defendants in the form of monies paid to Defendants for services.

139. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Class Members. Defendants also benefited from the receipt of Plaintiff and Class Members' PII, as Defendants used it in the course of its business.

140. The monies paid to Defendants for services involving Plaintiff and Class Members' PII were to be used by Defendants, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

141. Defendants also understood and appreciated that Plaintiff and Class Members' Private Information was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that Private Information.

142. But for Defendant's willingness and commitment to maintain privacy and confidentiality, that Private Information would not have been transferred to and untrusted with Defendants. Indeed, if Defendants had informed its patients that Defendant's data and cyber security measures were inadequate, Defendants would not have been permitted to continue to operate in that fashion by regulators, its shareholders, and its consumers.

143. As a result of Defendant's wrongful conduct, Defendants has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members.

Defendants continue to benefit and profit from their retention and use of the Private Information while its value to Plaintiff and Class Members has been diminished.

144. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this complaint, including compiling, using, and retaining Plaintiff and Class Members' Private Information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

145. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between the amount the value of their Private Information prior to and after the Data Breach.

146. Under principals of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendants failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

147. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds it received as a result of the conduct alleged herein.

COUNT IV
DECLARATORY JUDGMENT

148. Plaintiff re-alleges and incorporates by reference herein all of the previous allegations contained herein.

149. Defendants owe duties of care to Plaintiff and Class Members which require them to adequately secure their Private Information.

150. Defendants still possess Plaintiff and Class Members' Private Information.

151. Defendants donot specify in the Notice of Data Breach letters what steps they have taken to prevent a data security breach from occurring again.

152. Plaintiff and Class Members are at risk of harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

153. Plaintiff, therefore, seeks a declaration that (1) each of Defendant's existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect patients' personal information, and (2) to comply with their explicit or implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

(i) Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

(ii) Engaging third-party security auditors and internal personnel to run automated security monitoring;

(iii) Auditing, testing, and training its security personnel regarding any new or modified procedures;

(iv) Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

(v) Conducting regular database scanning and security checks;

(vi) Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

(vii) Purchasing credit monitoring services for Plaintiff and Class Members for a period of ten years; and

(viii) Meaningfully educating Plaintiff and Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Chris Cleveland, on behalf of herself and all Class Members, request judgment against Defendants and that the Court grant the following:

1. An order certifying the Class as defined herein, and appointing Plaintiff and his counsel to represent the Class;

2. An order enjoining Defendants from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of the Private Information belonging to Plaintiff and Class Members;

3. An order requiring Defendants to:

   a. Engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

   b. Engage third-party security auditors and internal personnel to run automated security monitoring;

   c. Audit, test, and train its security personnel regarding any new or modified procedures;

   d. Segment their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

   e. Conduct regular database scanning and security checks;

   f. Routinely and continually conduct internal training and education to inform internal security personnel how to

identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchase credit monitoring services for Plaintiff and Class Members for a period of ten years; and

h. Meaningfully educate Plaintiff and Class Members about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps they must take to protect themselves.

4. An order instructing Defendants to purchase or provide funds for credit monitoring services for Plaintiff and all Class Members;

5. An award of compensatory, statutory, nominal and punitive damages, in an amount to be determined at trial;

6. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

7. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

8. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, in here individual capacity and on behalf of all others similarly situated, hereby demands this matter be tried before a jury.

Respectfully submitted,

Dated: November 7, 2023

/s/Joshua Sanford
Joshua Sanford (AR #2001037)
SANFORD LAW FIRM, PLLC
10800 Financial Centre, Pkwy., Ste. 510
Little Rock, Arkansas 72211
Telephone: (501) 787-2040
josh@sanfordlaw.com

Bryan L. Bleichner (MN #0326689)*
Philip J. Krzeski (MN #0403291)*
CHESTNUT CAMBRONNE PA
100 Washington Avenue South
Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Facsimile: (612)-336-2940
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Attorneys for Plaintiff and the proposed Class

**Pro Hac Vice forthcoming*